

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11238017 A**(43) Date of publication of application: **31.08.99**

(51) Int. Cl.

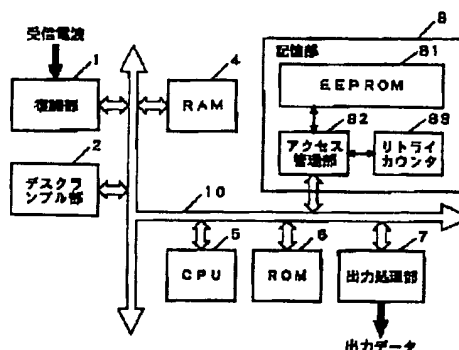
G06F 12/14
H04L 9/10(21) Application number: **10037802**(22) Date of filing: **19.02.98**(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**(72) Inventor: **USUKI IZUMI**(54) **RECEIVER**

COPYRIGHT: (C)1999,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a receiver protecting data at the time of illegal access to inner storage information and easily putting a part related to security in an unusable state at the time of abolishment.

SOLUTION: An access monitoring part 82 collates an access code requesting access to EEPROM 81 with a regular access code which the part 82 itself has when it receives the code and judges the matching/non-matching of the access codes. When the access codes are matched with each other by the judgment, access to EEPROM 81 is permitted. When they are not matched, the count value of a retry counter 83 is increased by one without permission and it waits again the input of the access code. When the count value arrives at a previously decided value, the retry counter 83 informs the access monitoring part 82 of the arrival. When the access monitoring part 82 judges the non-matching of the access codes after the notice, it deletes data in EEPROM 81.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-238017

(43) 公開日 平成11年(1999) 8月31日

(51) Int.Cl. ⁸	識別記号	F I
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14
H 0 4 L 9/10		H 0 4 L 9/00
		3 2 0 D
		6 2 1 Z

審査請求 未請求 請求項の数11 O L (全 11 頁)

(21) 出願番号 特願平10-37802

(22) 出願日 平成10年(1998) 2月19日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 薄木 泉

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

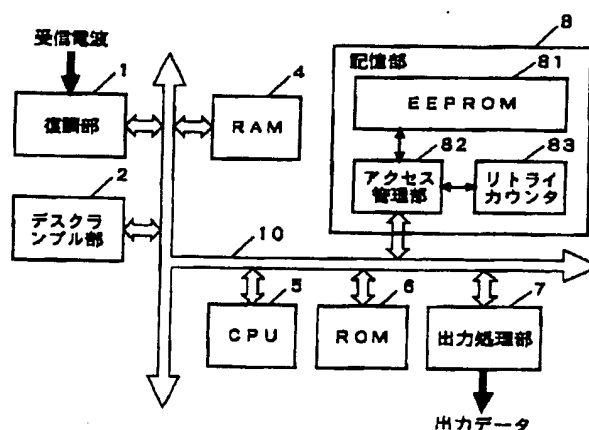
(74) 代理人 弁理士 小笠原 史朗

(54) 【発明の名称】 受信機

(57) 【要約】

【課題】 内部の記憶情報への不正アクセス時にデータを保護し、また廃棄時に容易にセキュリティに関する部分を使用不能な状態にする受信機を提供する。

【解決手段】 アクセス監視部82は、EEPROM81へのアクセスを要求するアクセスコードを受付けると、自らが持つ正規のアクセスコードとの照合を行いアクセスコードの一致／不一致を判断する。この判断でアクセスコードが一致した場合は、EEPROM81へのアクセスを許可するが、不一致の場合には、許可することなくリトライカウンタ83のカウント値を1つ増加させ、再びアクセスコードの入力を待つ。リトライカウンタ83は、カウント値が予め定めた値に達するとアクセス監視部82へその旨を通知する。アクセス監視部82は、この通知以後、さらにアクセスコードの不一致を判断した場合は、EEPROM81内のデータの消去を行う。



【特許請求の範囲】

【請求項1】 ダウンロードした受信データを電氣的書き換え可能な不揮発性半導体メモリ（以下、EEPROMという）に格納する受信機であって、

CPUと、

暗号化された受信データに対し、暗号解読を行うデスクランブル手段と、

前記暗号解読後のデータを格納する前記EEPROMと、

前記EEPROMに対して要求されるアクセスが正規なアクセスか不正なアクセスかを判断し、当該判断に応じて前記EEPROMへのアクセス許可／不許可を制御するアクセス監視手段と、

前記アクセス監視手段に対する不正なアクセスの回数をカウントし、当該カウントの値が予め定めた値に達した場合、前記アクセス監視手段へその旨を通知するリトライカウンタとを少なくとも備え、

前記アクセス監視手段は、前記リトライカウンタから前記通知があった場合、前記EEPROM内のデータを消去することを特徴とする、受信機。

【請求項2】 ダウンロードした受信データを電氣的書き換え可能な不揮発性半導体メモリ（以下、EEPROMという）に格納する受信機であって、

CPUと、

暗号化された受信データに対し、暗号解読を行うデスクランブル手段と、

前記暗号解読後のデータを格納する前記EEPROMと、

前記EEPROMに格納されているデータとは異なるデータが保存された偽データEEPROMと、

前記EEPROMに対して要求されるアクセスが正規なアクセスか不正なアクセスかを判断し、当該判断に応じて前記EEPROMまたは前記偽データEEPROMへのアクセス許可／不許可を制御するアクセス監視手段と、

前記アクセス監視手段に対する不正なアクセスの回数をカウントし、当該カウントの値が予め定めた値に達した場合、前記アクセス監視手段へその旨を通知するリトライカウンタとを少なくとも備え、

前記アクセス監視手段は、前記リトライカウンタから前記通知があった場合、前記偽データEEPROMに対するアクセス許可を行うことを特徴とする、受信機。

【請求項3】 前記アクセス監視手段は、前記偽データEEPROMに対するアクセス許可の後、さらに不正なアクセスがあった場合には、前記EEPROM内のデータを消去することを特徴とする、請求項2に記載の受信機。

【請求項4】 ダウンロードした受信データを電氣的書き換え可能な不揮発性半導体メモリ（以下、EEPROMという）に格納する受信機であって、

CPUと、

暗号化された受信データに対し、暗号解読を行うデスクランブル手段と、

前記暗号解読後のデータを格納する前記EEPROMと、

前記EEPROMに対して要求されるアクセスが正規なアクセスか不正なアクセスかを判断し、当該判断に応じて前記EEPROMへのアクセス許可／不許可を制御するアクセス監視手段と、

10 前記アクセス監視手段に対する不正なアクセスの回数をカウントし、当該カウントの値が予め定めた値に達した場合、前記アクセス監視手段へその旨を通知するリトライカウンタとを少なくとも備え、

前記アクセス監視手段は、前記リトライカウンタから前記通知があった場合、当該通知以後のアクセスを受付けないことを特徴とする、受信機。

【請求項5】 前記アクセス監視手段は、前記アクセスを受付けない状態に移した後であっても、アクセスを行う際の方法とは異なる予め定めた方法によりアクセスの受付けが可能な状態に復帰させることを特徴とする、請求項4に記載の受信機。

【請求項6】 前記アクセス監視手段は、前記異なる予め定めた方法において不正な行為が行われた場合には、前記EEPROM内のデータを消去することを特徴とする、請求項5に記載の受信機。

【請求項7】 受信データを前記EEPROMにダウンロードするための動作プログラムを別途記憶する記憶手段をさらに備え、

30 前記アクセス監視手段は、前記EEPROM内のデータを消去した場合、前記記憶手段に記憶している動作プログラムを前記EEPROMに読み出すとともに、同一の受信データを再び受信して前記EEPROMにダウンロードすることを特徴とする、請求項1または3若しくは6のいずれかに記載の受信機。

【請求項8】 データに固有の識別情報を付加するID付加手段をさらに備え、

前記EEPROMには、前記固有の識別情報を付加した後のデータを格納することを特徴とする、請求項1～7のいずれかに記載の受信機。

【請求項9】 前記デスクランブル手段は、電氣的に書き換え可能な素子を用いて回路が構成されており、前記アクセス監視手段は、前記リトライカウンタから前記通知があった場合、前記EEPROM内のデータを消去するとともに、前記デスクランブル手段の回路を消去することを特徴とする、請求項1～8のいずれかに記載の受信機。

【請求項10】 前記デスクランブル手段は、電氣的に書き換え可能な素子を用いて回路が構成されており、前記CPUは、外部からの指示に従って、前記EEPROM内のデータの消去、および前記デスクランブル手段

の回路の消去を行うことを特徴とする、請求項1～9のいずれかに記載の受信機。

【請求項11】 送信されるデータを受信し、当該受信したデータを内部に格納または外部へ出力する受信機であって、

送信されるデータを受信する受信手段と、
前記受信手段から出力されるデータに固有の識別情報を付加するID付加手段と、

前記固有の識別情報が付加されたデータを内部に格納または外部へ出力する処理手段とを少なくとも備える、受信機。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、受信機に関し、より特定的には、衛星通信システムやインターネット等において伝送されるデジタル画像、ソフトウェア等をダウンロードしたデータに対し、第三者の不正盗用を防止する受信機に関する。

【0002】

【従来の技術】図12に、従来の受信機の構成の一例として、デジタル衛星通信システム等で受信機として使用されるインテリジェント・レシーバー・デコーダ (Intelligent Receiver and Decoder) のブロック図を示す。図12において、従来の受信機は、復調部101と、デスクランブル部102と、ランダム・アクセス・メモリ (RAM) 104と、中央演算処理装置 (CPU) 105と、リード・オンリー・メモリ (ROM) 106と、出力処理部107と、EEPROM (Electrically Erasable and Programmable ROM) 181とを備える。これらの各構成は、バス110により相互に接続されている。

【0003】衛星から受信した電波は、復調部101でデジタル符号データに変換される。変換されたデジタル符号データは、デスクランブル部102において予め定めた規則の下暗号を解読される。暗号解読後のデータは、通常、RAM104に一旦格納され（ただし、受信データが連続している場合には、RAM104に格納することなく直ちに出力処理部7を介して出力することもある）、その後、出力処理部107を介してテレビ受像器やパーソナル・コンピュータ等の外部端末（以下、外部PCと称する）へ出力される（図示せず）。ここで、受信データが受信機のシステムソフトダウンロード用のデータであった場合、CPU105は、RAM104に格納された暗号解読後のデータをさらにEEPROM181に記憶する。

【0004】なお、上記受信データが、例えば、MPEG2 (Moving Picture Experts Group 2) 方式のデータである場合には、暗号解読後に内蔵するMPEG2デコード部（図示せず）によってデータがデコードされる。

【0005】このように、通常、データはメモリ (RA 50

M104, EEPROM181) に格納され、その後外部PCに出力する等、ユーザが自由に使用することができる。特に、衛星通信における上記従来の受信機では、システムソフトは、衛星回線からのダウンロードによっていつでも更新が可能なようにEEPROM181に格納されている。

【0006】

【発明が解決しようとする課題】上述したように、従来の受信機は、受信したデータをメモリに格納している。しかし、従来の受信機は、これらの格納データに対し何らセキュリティ対策を施していないため、第三者の不正アクセスにより格納データが容易にコピーされてしまう。特に、コピーされた格納データが著作権のあるデータの場合には、著作権侵害等の問題が発生してしまう。

【0007】また、受信機内のEEPROM181に格納されているデータは、受信機を分解して直接EEPROM181を読み出すことによっても第三者が自由に得ることができ、これによっても著作権侵害等の問題が発生してしまう。このため、通常、受信機の廃棄の際には、廃棄物を解析されても問題がないように受信機のセキュリティに関連するデバイスを完全に使用不能状態にしてから廃棄する。しかし、このようにデバイスを完全に使用不能状態にするには、手間やコストがかかる等の問題がある。

【0008】それ故、本発明の目的は、受信機内に記憶している情報への不正アクセス時にデータを保護し、また、廃棄時に容易にセキュリティに関する部分を使用不能な状態にすることが可能な受信機を提供することである。

【0009】

【課題を解決するための手段および発明の効果】第1の発明は、ダウンロードした受信データを電氣的書き換え可能な不揮発性半導体メモリ（以下、EEPROMという）に格納する受信機であって、CPUと、暗号化された受信データに対し、暗号解読を行うデスクランブル手段と、暗号解読後のデータを格納するEEPROMと、EEPROMに対して要求されるアクセスが正規なアクセスか不正なアクセスかを判断し、当該判断に応じてEEPROMへのアクセス許可／不許可を制御するアクセス監視手段と、アクセス監視手段に対する不正なアクセスの回数をカウントし、当該カウントの値が予め定めた値に達した場合、アクセス監視手段へその旨を通知するリトライカウンタとを少なくとも備え、アクセス監視手段は、リトライカウンタから通知があった場合、EEPROM内のデータを消去することを特徴とする。

【0010】上記のように、第1の発明によれば、第三者の不正アクセスがあった場合、予め定めた回数に達すると自動的にEEPROM内のデータを消去する。これにより、第三者への情報の漏洩防止を図ることができる。

【0011】第2の発明は、ダウンロードした受信データを電氣的書き換え可能な不揮発性半導体メモリ（以下、EEPROMという）に格納する受信機であって、CPUと、暗号化された受信データに対し、暗号解読を行うデスクランブル手段と、暗号解読後のデータを格納するEEPROMと、EEPROMに格納されているデータとは異なるデータが保存された偽データEEPROMと、EEPROMに対して要求されるアクセスが正規なアクセスか不正なアクセスかを判断し、当該判断に応じてEEPROMまたは偽データEEPROMへのアクセス許可／不許可を制御するアクセス監視手段と、アクセス監視手段に対する不正なアクセスの回数をカウントし、当該カウントの値が予め定めた値に達した場合、アクセス監視手段へその旨を通知するリトライカウンタとを少なくとも備え、アクセス監視手段は、リトライカウンタから通知があった場合、偽データEEPROMに対するアクセス許可を行うことを特徴とする。

【0012】上記のように、第2の発明によれば、第三者の不正アクセスがあった場合、予め定めた回数に達すると自動的に偽データを出力する。これにより、EEPROM内のデータを消去することなく、第三者への情報の漏洩防止を図ることができる。

【0013】第3の発明は、第2の発明において、アクセス監視手段は、偽データEEPROMに対するアクセス許可の後、さらに不正なアクセスがあった場合には、EEPROM内のデータを消去することを特徴とする。

【0014】上記のように、第3の発明によれば、第2の発明において、出力したデータが偽データであると判断されても、その後不正アクセスがあった場合には、自動的にEEPROM内のデータを消去する。従って、第1の発明と同様に、確実に第三者への情報の漏洩防止を図ることができる。

【0015】第4の発明は、ダウンロードした受信データを電氣的書き換え可能な不揮発性半導体メモリ（以下、EEPROMという）に格納する受信機であって、CPUと、暗号化された受信データに対し、暗号解読を行うデスクランブル手段と、暗号解読後のデータを格納するEEPROMと、EEPROMに対して要求されるアクセスが正規なアクセスか不正なアクセスかを判断し、当該判断に応じてEEPROMへのアクセス許可／不許可を制御するアクセス監視手段と、アクセス監視手段に対する不正なアクセスの回数をカウントし、当該カウントの値が予め定めた値に達した場合、アクセス監視手段へその旨を通知するリトライカウンタとを少なくとも備え、アクセス監視手段は、リトライカウンタから通知があった場合、当該通知以後のアクセスを受け付けないことを特徴とする。

【0016】上記のように、第4の発明によれば、第三者の不正アクセスがあった場合、予め定めた回数に達するとアクセスを受け付けない状態にする。これにより、第

三者への情報の漏洩防止を図ることができる。

【0017】第5の発明は、第4の発明において、アクセス監視手段は、アクセスを受け付けない状態に遷移した後であっても、アクセスを行う際の方法とは異なる予め定めた方法によりアクセスの受け付けが可能な状態に復帰させることを特徴とする。

【0018】上記のように、第5の発明によれば、第4の発明において、アクセスする方法とは異なる方法を用いて状態を復帰できるようにする。これにより、正規のユーザは、容易に元の状態に復帰させることができる。

【0019】第6の発明は、第5の発明において、アクセス監視手段は、異なる予め定めた方法において不正な行為が行われた場合には、EEPROM内のデータを消去することを特徴とする。

【0020】上記のように、第6の発明によれば、第5の発明において、異なる方法の存在を知られても不正な行為を行った場合には、自動的にEEPROM内のデータを消去する。従って、第1の発明と同様に、確実に第三者への情報の漏洩防止を図ることができる。

【0021】第7の発明は、第1、第3および第6の発明において、受信データをEEPROMにダウンロードするための動作プログラムを別途記憶する記憶手段をさらに備え、アクセス監視手段は、EEPROM内のデータを消去した場合、記憶手段に記憶している動作プログラムをEEPROMに読み出すとともに、同一の受信データを再び受信してEEPROMにダウンロードすることを特徴とする。

【0022】上記のように、第7の発明によれば、第1、第3および第6の発明において、ダウンロードに必要な動作プログラムを記録した記憶手段をさらに備えている。これにより、EEPROM内のデータを消去しても、その後、記憶手段から動作プログラムを読み込むことにより消去したデータを復元することができる。

【0023】第8の発明は、第1～第7の発明において、データに固有の識別情報を付加するID付加手段をさらに備え、EEPROMには、固有の識別情報を付加した後のデータを格納することを特徴とする。

【0024】上記のように、第8の発明によれば、第1～第7の発明において、データに固有の識別情報を付加するID付加手段をさらに備える。これにより、万データが不正に盗用されたとしても、付加された固有の識別情報から盗用データであると判断することができる。従って、第三者の不正行為の摘発が容易になり、ひいては事前に不正行為を抑制するという効果がある。

【0025】第9の発明は、第1～第8の発明において、デスクランブル手段は、電氣的に書き換え可能な素子を用いて回路が構成されており、アクセス監視手段は、リトライカウンタから通知があった場合、EEPROM内のデータを消去するとともに、デスクランブル手段の回路を消去することを特徴とする。

【0026】上記のように、第9の発明によれば、第1～第8の発明において、デスクランブル手段の回路を電氣的に書き換え可能な素子を用いて構成する。そして、第三者の不正アクセスがあった場合、予め定めた回数に達すると自動的にEEPROM内のデータを消去し、かつ、デスクランブル手段の回路を電氣的に消去する。これにより、第三者への情報の漏洩防止を図ることができる。また、セキュリティに関連する情報の漏洩防止を図ることができる。

【0027】第10の発明は、第1～第9の発明において、デスクランブル手段は、電氣的に書き換え可能な素子を用いて回路が構成されており、CPUは、外部からの指示に従って、EEPROM内のデータの消去、およびデスクランブル手段の回路の消去を行うことを特徴とする。

【0028】上記のように、第10の発明によれば、第1～第9の発明において、デスクランブル手段の回路を電氣的に書き換え可能な素子を用いて構成する。そして、外部からの指示によりEEPROM内のデータの消去、およびデスクランブル手段の回路の電氣的消去を行えるようにする。これにより、廃棄時においても、確実にセキュリティに関連する情報の漏洩防止を図ることができる。

【0029】第11の発明は、送信されるデータを受信し、当該受信したデータを内部に格納または外部へ出力する受信機であって、送信されるデータを受信する受信手段と、受信手段から出力されるデータに固有の識別情報を付加するID付加手段と、固有の識別情報が付加されたデータを内部に格納または外部へ出力する処理手段とを少なくとも備える。

【0030】上記のように、第11の発明によれば、データに固有の識別情報を付加した後、内部に格納または外部へ出力する。これにより、データがどの受信機から取得されたものかを判断することができる。従って、第三者の不正行為を事前に抑制するとともに、第三者の不正行為があった場合は摘発が容易になる。

【0031】

【発明の実施の形態】以下、本発明の実施形態について、デジタル衛星通信システム等で受信機として使用されるインテリジェント・レシーバー・デコーダを一例に挙げて説明する。

【0032】（第1の実施形態）図1は、本発明の第1の実施形態に係る受信機の構成を示すブロック図である。図1において、本第1の実施形態に係る受信機は、復調部1と、デスクランブル部2と、RAM4と、CPU5と、ROM6と、出力処理部7と、記憶部8とを備える。これらの各構成は、バス10によって相互に接続されている。また、記憶部8は、EEPROM81と、アクセス監視部82と、リトライカウンタ83とを備える。

【0033】復調部1は、受信データをデジタル符号データに変換する。デスクランブル部2は、復調部1でデジタル符号化したデータの暗号を解読する。RAM4は、データを格納する。CPU5は、受信機全体の制御を行う。また、CPU5は、アクセスに必要な予め定めたアクセスコードを記憶している。ROM6は、受信機が行う制御プログラムを格納している。出力処理部7は、デスクランブル部2の出力をテレビ受像器等（図示せず）へ出力する。EEPROM81は、上記受信データが受信機のシステムソフトダウンロード用のデータであった場合、当該データを記憶する。アクセス監視部82は、アクセスに必要な予め定めたアクセスコードを記憶している。なお、上記CPU5が記憶するアクセスコードとアクセス監視部82が記憶するアクセスコードとは同じものである。リトライカウンタ83は、アクセス監視部82が行うアクセスコードの照合回数をカウントする。

【0034】衛星から電波として受信されたデータは、復調部1においてデジタル符号データに変換される。変換されたデジタル符号データは、デスクランブル部2において予め定めた規則の下、暗号が解読される。暗号解読後のデータは、通常、RAM4に一旦格納され（ただし、受信データが連続している場合には、RAM4に格納することなく直ちに出力処理部7を介して出力することもある）、その後、出力処理部7を介して外部PC（図示せず）へ出力される。なお、上記受信データが、例えば、MPEG2方式のデータである場合には、内蔵するMPEG2デコード部（図示せず）によって暗号解読後のデータがデコードされる。

【0035】ここで、受信データが受信機のシステムソフトダウンロード用のデータであった場合、CPU5は、RAM4に格納された暗号解読後のデータをさらにEEPROM81に記憶すべく、アクセス監視部82へアクセスを行う。

【0036】このCPU5とアクセス監視部82との間のアクセスは、まず、CPU5が自らが記憶するアクセスコードを、アクセス監視部82へ通知する。そして、アクセス監視部82は、CPU5から通知されたアクセスコードと、アクセス監視部82自らが記憶しているアクセスコードとを照合し、一致した場合にのみEEPROM81へのアクセスを許可する。従って、正常なアクセスの場合には、CPU5およびEEPROM81の双方のアクセスコードが同一であるため、問題なくアクセスが可能となる。

【0037】一方、不正行為を行う第三者は、自らの機器（以下、不正機器と称する）を使用してEEPROM81の内容を読み取ろうとする。この場合、第三者が行うアクセスは、不正機器内のCPUを使用して行われることになる。従って、このような不正行為が行われても、不正機器内のCPUがアクセスコードを通知する必

要があることを知らないため、また、通知する必要があること知っていても不正機器のCPUが固有に記憶する誤ったアクセスコードであるため、アクセス監視部82がこのアクセスを拒絶する(アクセスコードを照合しても、一致しないからである)。これに対して、第三者は、何回か異なる任意のアクセスコードを試みると考えられる。しかし、リトライカウンタ83は、アクセス監視部82がアクセスを拒絶した回数をカウントしており、予め定めた回数が行われたときにはアクセス監視部82へその旨を通知する。この通知を受けたアクセス監視部82は、最終的な対応として、EEPROM81内の格納データを消去する。

【0038】このように、アクセスを試みることができる回数を予め制限することで、不正行為を行う第三者のアクセスコードが正規のアクセスコードと合致する確率をきわめて低くできる(もちろん、アクセスコードのビット数にも関係する)。

【0039】以下、上記構成による第1の実施形態に係る受信機の不正アクセスに対する動作を、図2を参照しつつ説明する。図2は、本発明の第1の実施形態に係る受信機における状態遷移を示す図である。図2においては、リトライカウンタ83がアクセス監視部82へ通知を行うカウント数を「3」としている。

【0040】まず、初期状態として、アクセス監視部82は、アクセスコードを受け付ける第1のアクセスコード待ち状態にある(状態S1)。また、リトライカウンタ83は、初期値「0」とであるとする。ある者がアクセスを試みる(トライ)、すなわち、アクセスコードが通知されてくると、アクセス監視部82は、通知されたアクセスコードと自ら記憶しているアクセスコードとを照合する。ここで、通知されたアクセスコードが正規のものである場合、アクセス監視部82は、アクセスを許可する。

【0041】一方、通知されたアクセスコードが不正なものである場合、アクセス監視部82は、アクセスコード不一致と判断し、リトライカウンタ83を1つ増加させ「1」とする。このときは、まだ状態S1にあり、再びアクセスコードを受け付ける状態となる。再び不正アクセスコードが入力されると、アクセス監視部82は、またアクセスコード不一致と判断し、さらにリトライカウンタ83を1つ増加させ「2」とする。同様に、状態S1において、再び不正アクセスコードが入力されると、アクセス監視部82は、アクセスコード不一致と判断し、さらにリトライカウンタ83を1つ増加させ「3」とする。ここで、リトライカウンタ83のカウント値が「3」に達したため、リトライカウンタ83は、アクセス監視部82へその旨を通知する。アクセス監視部82は、この通知を受けて第2のアクセスコード待ち状態へ遷移する(状態S2)。

【0042】状態S2において、再び不正アクセスコー

ドが入力されると、アクセス監視部82は、アクセスコード不一致と判断するとともに、EEPROM81内の格納データを消去する(状態S3)。一方、状態S2において、正規のアクセスコードが入力された場合は、アクセス監視部82は、アクセスを許可するとともに、状態S1へ遷移させ、さらにリトライカウンタ83のカウント値をリセットする。

【0043】以上のように、本発明の第1の実施形態に係る受信機は、不正アクセスの回数をカウントし、予め定めた回数が行われた場合には、EEPROM81内の格納データを消去する。これにより、アクセスコードを知らない第三者の不正アクセス行為があった場合、データ漏洩防止を図ることができる。

【0044】(第2の実施形態)図3は、本発明の第2の実施形態に係る受信機の構成を示すブロック図である。図3において、本第2の実施形態に係る受信機は、復調部1と、デスクランブル部2と、RAM4と、CPU5と、ROM6と、出力処理部7と、記憶部8aとを備える。これらの各構成は、バス10によって相互に接続されている。また、記憶部8aは、EEPROM81と、アクセス監視部82と、リトライカウンタ83と、偽データEEPROM84とを備える。

【0045】図3に示すように、本第2の実施形態に係る受信機の記憶部8aは、上記第1の実施形態に係る受信機の記憶部8に偽データEEPROM84をさらに加えた構成である。偽データEEPROM84は、EEPROM81に格納しているデータとは異なる偽のデータを格納している。なお、本第2の実施形態に係る受信機のその他の構成は、上記第1の実施形態に係る受信機の構成と同様であり、当該構成については同一の参照番号を付してその説明を省略する。

【0046】第2の実施形態に係る受信機は、アクセス監視部82がリトライカウンタ83から通知を受けた場合、最終的な対応としてEEPROM81内の格納データを消去する前に、偽データを出力する。

【0047】以下、上記構成による第2の実施形態に係る受信機の不正アクセスに対する動作を、図4を参照しつつ説明する。図4は、本発明の第2の実施形態に係る受信機における状態遷移を示す図である。図4においては、リトライカウンタ83がアクセス監視部82へ通知を行うカウント数を「3」としている。なお、状態S1および状態S3は、上記第1の実施形態に係る受信機の場合と同様であるため、その説明は省略する。

【0048】リトライカウンタ83は、カウント値が「3」に達するとアクセス監視部82へその旨を通知する。アクセス監視部82は、この通知を受けて、外部からはあたかも正規のアクセスコードに合致したかのように偽データEEPROM84に格納している偽データを出力する(状態S4)。

【0049】このとき、第三者が偽データだと気づい

て、再び不正アクセスコードが入力されると、アクセス監視部82は、アクセスコード不一致と判断するとともに、EEPROM81内の格納データを消去する(状態S3)。一方、状態S4において、正規のアクセスコードが入力された場合は、アクセス監視部82は、アクセスを許可するとともに、状態S4から状態S1へ遷移させ、さらにリトライカウンタ83のカウント値をリセットする。

【0050】なお、状態S4から状態S3への遷移は、1回の不正アクセスですぐに行うようにするほか、状態S1から状態S4への遷移と同様に、リトライカウンタ83を使用して予め定めた回数の不正アクセスがあった場合に行うようにしてもよい(図11を参照)。

【0051】以上のように、本発明の第2の実施形態に係る受信機は、不正アクセスの回数をカウントし、予め定めた回数が行われた場合には、EEPROM81内の格納データを消去する前に、まず偽のデータを出力する。これにより、アクセスコードを知らない第三者の不正アクセス行為があった場合、格納データの消去を極力避けつつもデータ漏洩防止を図ることができる。

【0052】(第3の実施形態)図5は、本発明の第3の実施形態に係る受信機の構成を示すブロック図である。図5において、本第3の実施形態に係る受信機は、復調部1と、デスクランブル部2と、RAM4と、CPU5と、ROM6と、出力処理部7と、記憶部8とを備える。これらの各構成は、バス10によって相互に接続されている。また、記憶部8は、EEPROM81と、アクセス監視部82と、リトライカウンタ83とを備える。

【0053】図5に示すように、本第3の実施形態に係る受信機は、構成的には上記第1の実施形態に係る受信機と同様の構成である。本第3の実施形態に係る受信機が上記第1の実施形態に係る受信機と異なる点は、図2における状態S2で行う処理である。なお、本第3の実施形態に係る受信機のその他の構成は、上記第1の実施形態に係る受信機の構成と同様であり、当該構成については同一の参照番号を付してその説明を省略する。

【0054】以下、上記構成による第3の実施形態に係る受信機の不正アクセスに対する動作を、図6を参照しつつ説明する。図6は、本発明の第3の実施形態に係る受信機における状態遷移を示す図である。図6においては、リトライカウンタ83がアクセス監視部82へ通知を行うカウント数を「3」としている。なお、状態S1および状態S3は、上記第1の実施形態に係る受信機の場合と同様であるため、その説明は省略する。

【0055】リトライカウンタ83は、カウント値が「3」に達するとアクセス監視部82へその旨を通知する。アクセス監視部82は、この通知を受けて、アクセスコードの受け付けを完全に拒絶する(状態S5)。ここで、この状態S5にある場合、復帰コード(アクセスコ

ードとは別の信号線を規定の状態にするコード)の入力により復帰できるようにする。すなわち、状態S5において、正規のアクセスコードが入力された場合には、状態S1へ遷移するようにする。一方、第三者が復帰コードの存在を知っていても、正規の復帰コードまでを知り得ることは希であり、不正な復帰コードで再び試みた場合には、上記と同様にEEPROM81内の格納データを消去する(状態S3)。このような処理を行うことで、状態S5のまま第三者が不正アクセスを断念した場合には、正規のユーザが復帰コードを入力することで、容易に状態S1へ遷移させることができる。

【0056】なお、状態S5から状態S3への遷移は、1回の不正な復帰コードの入力によりすぐに行うようにする他、状態S1から状態S5への遷移と同様に、リトライカウンタ83を使用して予め定めた回数の不正な復帰コードの入力があった場合に行うようにしてもよい。

【0057】以上のように、本発明の第3の実施形態に係る受信機は、不正アクセスの回数をカウントし、予め定めた回数が行われた場合には、アクセスを完全に拒絶し、極秘の復帰コードの受け付け状態にする。これにより、アクセスコードを知らない第三者の不正アクセス行為があった場合、格納データの消去を極力避けつつもデータ漏洩防止を図ることができる。

【0058】(第4の実施形態)図7は、本発明の第4の実施形態に係る受信機の構成を示すブロック図である。図7において、本第4の実施形態に係る受信機は、復調部1と、デスクランブル部2と、RAM4と、CPU5と、ROM6と、出力処理部7と、記憶部8とを備える。これらの各構成は、バス10によって相互に接続されている。また、記憶部8は、EEPROM81と、アクセス監視部82と、リトライカウンタ83とを備える。

【0059】図7に示すように、本第4の実施形態に係る受信機は、構成的には上記第1の実施形態に係る受信機と同様の構成である。本第4の実施形態に係る受信機が上記第1の実施形態に係る受信機と異なるのは、ROM6内にダウンロードに関するソフトウェアのすべて(以下、ダウンロードモジュールという)を格納する部分DM61を有している点である。このDM61へのダウンロードモジュールの格納は、例えば、受信機の出荷段階で行えばよい。なお、本第5の実施形態に係る受信機のその他の構成は、上記第1の実施形態に係る受信機の構成と同様であり、当該構成については同一の参照番号を付してその説明を省略する。

【0060】以下、上記構成による第5の実施形態に係る受信機の不正アクセスに対する動作を説明する。リトライカウンタ83は、カウント値が「3」に達するとアクセス監視部82へその旨を通知する。アクセス監視部82は、この通知を受けて、第2のアクセスコード待ち状態へ遷移する(図2における状態S2を参照)。状態

S 2において、再び不正アクセスコードが入力されると、アクセス監視部82は、アクセスコード不一致と判断するとともに、EEPROM81内の格納データを消去する。その後、アクセス監視部82は、ダウンロードモジュールをROM6内のDM61から読み出して再びEEPROM81内に格納する処理を自動的に行う。

【0061】以上のように、本発明の第4の実施形態に係る受信機は、不正アクセスの回数をカウントし、予め定めた回数が行われた場合には、EEPROM81内の格納データを消去する。そして、その後、消去した格納データのうちダウンロードモジュールのみを自動的に復元する。これにより、アクセスコードを知らない第三者の不正アクセス行為によりEEPROM81内の格納データが消去された場合でも、衛星から送られてくる同一データを再び受信してEEPROM81に再格納することで、容易に消去データの復元を行うことができる。

【0062】なお、本第4の実施形態において示したROM6内のDM61にダウンロードモジュールを格納する構成は、上記第1の実施形態に係る受信機のみならず上記第2および第3の実施形態に係る受信機においても同様に用いることが可能である。

【0063】(第5の実施形態)図8は、本発明の第5の実施形態に係る受信機の構成を示すブロック図である。図8において、本第5の実施形態に係る受信機は、復調部1と、デスクランブル部2と、RAM4と、CPU5と、ROM6と、出力処理部7と、記憶部8と、ID (identification) 付加部9とを備える。これらの各構成は、バス10によって相互に接続されている。また、記憶部8は、EEPROM81と、アクセス監視部82と、リトライカウンタ83とを備える。

【0064】図8に示すように、本第5の実施形態に係る受信機は、上記第1の実施形態に係る受信機に、ID付加部3を加えたものである。ID付加部3は、受信機固有のID情報を電子すかしの手法で受信データ内に埋め込む処理を行う。なお、本第5の実施形態に係る受信機のその他の構成は、上記第1の実施形態に係る受信機の構成と同様であり、当該構成については同一の参照番号を付してその説明を省略する。

【0065】ID付加部3においてID情報を埋め込むデータは、RAM4に格納される前のデータであってもよいし、外部PC等へ出力する際にRAM4から読み出されるデータであってもよい。

【0066】以上のように、本発明の第5の実施形態に係る受信機は、データ保護の処理を行う前に受信データに受信機固有のID情報を埋め込む。これにより、万一アクセスコードが一致して第三者に不正にデータが盗用されても、埋め込まれたID情報からデータが不正盗用されたものであるという判断ができる。従って、第三者の不正行為の摘発が容易になり、ひいては事前に不正行為を抑制するという効果がある。

【0067】なお、本第5の実施形態において示した受信データに受信機固有のID情報を埋め込む手法は、上記第1の実施形態に係る受信機のみならず上記第2～第4の実施形態に係る受信機においても同様に用いることが可能である。また、本第5の実施形態において示した受信データに受信機固有のID情報を埋め込む手法は、必ずしも上記第1～第4の実施形態とともに使用しなければならないものではなく、事前に不正行為を抑制するという意味において単独で用いることも可能である。

10 【0068】(第6の実施形態)図9は、本発明の第6の実施形態に係る受信機の構成を示すブロック図である。図9において、本第6の実施形態に係る受信機は、復調部1と、FPGA(Field Programmable gate array) デスクランブル部2aと、RAM4と、CPU5と、ROM6と、出力処理部7と、記憶部8とを備える。これらの各構成は、バス10によって相互に接続されている。また、記憶部8は、EEPROM81と、アクセス監視部82と、リトライカウンタ83とを備える。

20 【0069】図9に示すように、本第6の実施形態に係る受信機は、上記第1の実施形態に係る受信機のデスクランブル部2を、FPGAデスクランブル部2aに代えたものである。また、FPGAデスクランブル部2aの内部回路を書き換えるための専用の信号線26が、アクセス監視部82からFPGAデスクランブル部2aへ接続されている。なお、本第6の実施形態に係る受信機のその他の構成は、上記第1の実施形態に係る受信機の構成と同様であり、当該構成については同一の参照番号を付してその説明を省略する。

30 【0070】FPGAデスクランブル部2aとは、FPGAによって回路構成されたデスクランブル部である。そして、FPGAとは、外部からの電気的処理により回路プログラムが可能なゲートアレーをいう。従って、FPGA回路は、電気的に消去することも可能なのである。

【0071】以下、上記構成による第6の実施形態に係る受信機の不正アクセスに対する動作を説明する。リトライカウンタ83は、カウント値が「3」に達するとアクセス監視部82へその旨を通知する。アクセス監視部82は、この通知を受けて、第2のアクセスコード待ち状態へ遷移する(図2における状態S2を参照)。状態S2において、再び不正アクセスコードが入力されると、アクセス監視部82は、アクセスコード不一致と判断するとともに、EEPROM81内の格納データを消去し、かつ、信号線26を使用してFPGAデスクランブル部2aのFPGA回路データを消去する。

【0072】以上のように、本発明の第6の実施形態に係る受信機は、デスクランブル部をFPGA回路で構成する。さらに、不正アクセスの回数をカウントし、予め定めた回数が行われた場合には、EEPROM81内の

格納データとともにFPGAデスクランブル部2aのFPGA回路データをも消去する。これにより、アクセスコードを知らない第三者の不正アクセス行為があった場合、EEPROM81内の格納データを消去することによりデータ漏洩防止を図るとともに、暗号解読を行うFPGAデスクランブル部2aの回路をも消去するため、セキュリティに関連する情報の漏洩防止も図ることができる。

【0073】なお、本第6の実施形態において示したデスクランブル部をFPGA回路によって構成することは、上記第1の実施形態に係る受信機のみならず上記第2～第5の実施形態に係る受信機においても同様に用いることが可能である。

【0074】(第7の実施形態)図10は、本発明の第7の実施形態に係る受信機の構成を示すブロック図である。図10において、本第7の実施形態に係る受信機は、復調部1と、FPGAデスクランブル部2aと、RAM4と、CPU5と、ROM6と、出力処理部7と、記憶部8とを備える。これらの各構成は、バス10によって相互に接続されている。また、記憶部8は、EEPROM81と、アクセス監視部82と、リトライカウンタ83とを備える。

【0075】図10に示すように、本第7の実施形態に係る受信機は、上記第1の実施形態に係る受信機のデスクランブル部2を、FPGAデスクランブル部2aに代えたものである。また、FPGAデスクランブル部2aの内部回路を書き換えるための専用の信号線27が、CPU5からFPGAデスクランブル部2aへ接続されている。なお、本第7の実施形態に係る受信機のその他の構成は、上記第1の実施形態に係る受信機の構成と同様であり、当該構成については同一の参照番号を付してその説明を省略する。

【0076】上記構成による第7の実施形態に係る受信機は、不正アクセスに対するデータ保護動作は上記第1～第6の実施形態に係る受信機と同様であるが、廃棄時の処理が異なる。すなわち、受信機の廃棄時に、CPU5から再度EEPROM81内の格納データを消去するとともに、信号線27を使用してFPGAデスクランブル部2aのFPGA回路データを消去するのである。

【0077】以上のように、本発明の第7の実施形態に係る受信機は、デスクランブル部をFPGA回路で構成する。そして、受信機の廃棄時には、CPU5からEEPROM81内の格納データおよびFPGAデスクランブル部2aのFPGA回路データの消去を行う。これにより、セキュリティに関連するデータおよび機能をすべて使用不能とした後に受信機を廃棄することができ、セキュリティに関連する情報の漏洩防止をより確実に図ることができる。

【0078】なお、本第7の実施形態において示したE

EEPROM81内の格納データおよびFPGAデスクランブル部2aのFPGA回路データを受信機の廃棄時に消去する処理は、上記第1の実施形態に係る受信機のみならず上記第2～第6の実施形態に係る受信機においても同様に用いることが可能である。

【0079】また、本発明に係る受信機は、上記第1～第7の実施形態で示したように無線の通信システムにのみ用いられるものではなく、インターネット等の有線による通信システムにも同様に用いることができる。

10 【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る受信機の構成を示すブロック図である。

【図2】本発明の第1の実施形態に係る受信機における状態遷移を示す図である。

【図3】本発明の第2の実施形態に係る受信機の構成を示すブロック図である。

【図4】本発明の第2の実施形態に係る受信機における状態遷移を示す図である。

【図5】本発明の第3の実施形態に係る受信機の構成を示すブロック図である。

【図6】本発明の第3の実施形態に係る受信機における状態遷移を示す図である。

【図7】本発明の第4の実施形態に係る受信機の構成を示すブロック図である。

【図8】本発明の第5の実施形態に係る受信機の構成を示すブロック図である。

【図9】本発明の第6の実施形態に係る受信機の構成を示すブロック図である。

【図10】本発明の第7の実施形態に係る受信機の構成を示すブロック図である。

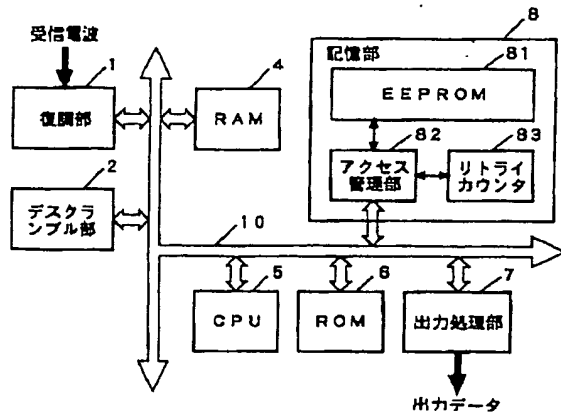
【図11】他の状態遷移の一例を示す図である。

【図12】従来の受信機の構成の一例を示すブロック図である。

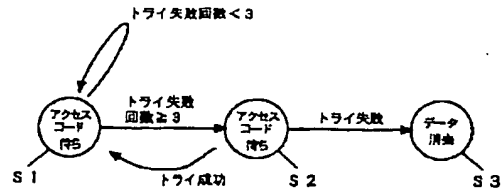
【符号の説明】

- 1、101…復調部
- 2、2a、102…デスクランブル部
- 3…ID付加部
- 4、104…RAM
- 5、105…CPU
- 6、106…ROM
- 7、107…出力処理部
- 8、8a…記憶部
- 10、110…バス
- 26、27…信号線
- 61…ダウンロードモジュール(DM)
- 81、181…EEPROM
- 82…アクセス監視部
- 83…リトライカウンタ
- 84…偽データEEPROM

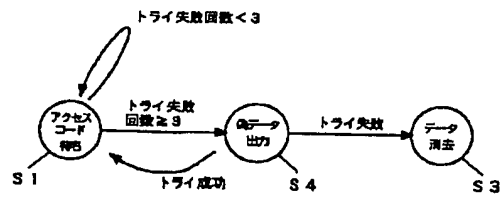
【図1】



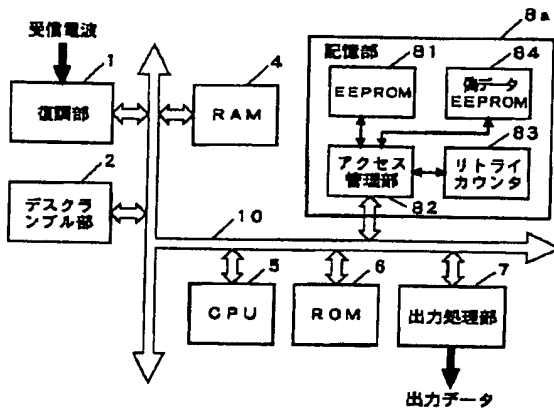
【図2】



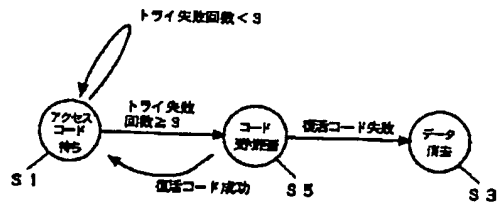
【図4】



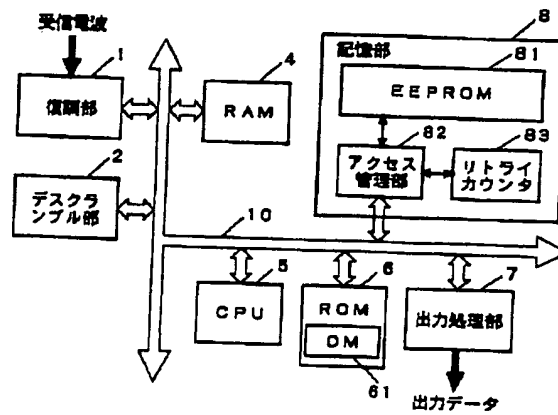
【図3】



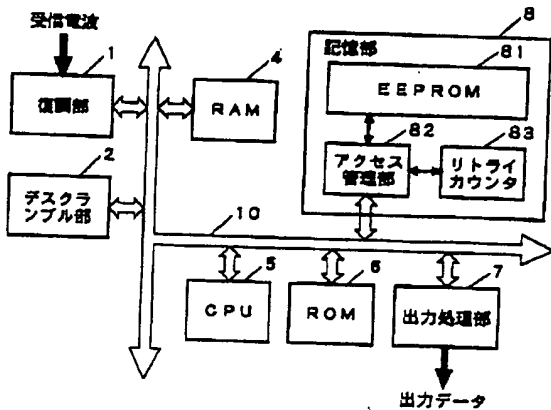
【図6】



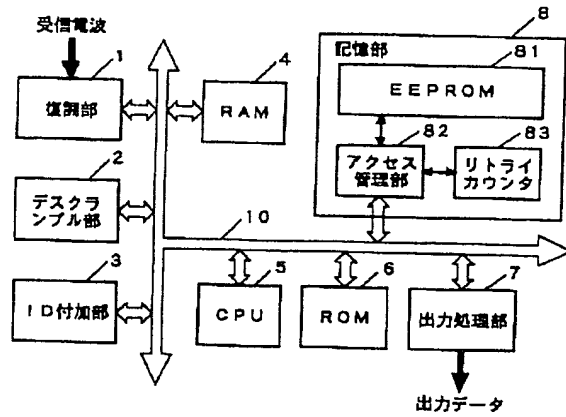
【図7】



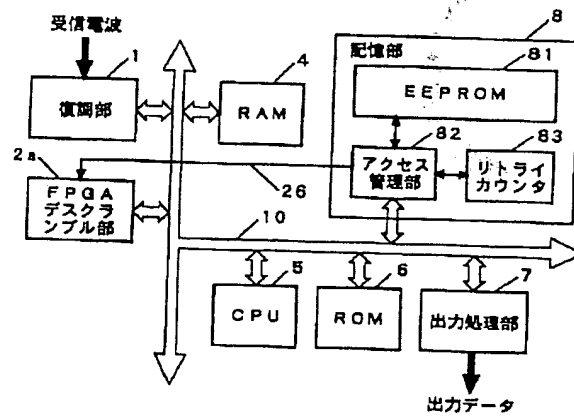
【図5】



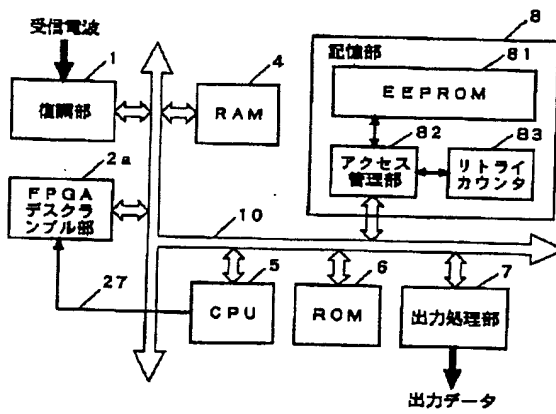
【図8】



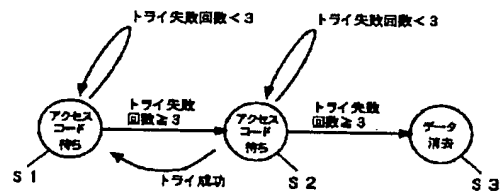
【図9】



【図10】



【図11】



【図12】

